

Державний вищий навчальний заклад
Донецький національний технічний університет
Кафедра прикладної математики та інформатики

«ЗАТВЕРДЖУЮ»

Перший проректор

_____ Леонід БАЧУРІН

«_____» _____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ОНД 2.09 БЕЗПЕКА ТА ЗАХИСТ ОПЕРАЦІЙНИХ СИСТЕМ

(шифр і назва навчальної дисципліни)

Рівень освіти: перший (бакалаврський)

Спеціальність

125 Кібербезпека

(шифр і назва спеціальності (тей))

Освітня програма

Кібербезпека та захист інформації

(назва освітньої програми)

Мова навчання: українська

Робоча програма навчальної дисципліни «Безпека та захист операційних систем»
(повна назва дисципліни)

для здобувачів вищої освіти за спеціальністю 125 Кібербезпека «30» 08 2023 року. – 10 с.

Розробник:

Ярослав ДОРОГИЙ, д.т.н., проф.,

Робоча програма затверджена на засіданні кафедри прикладної математики та інформатики

Протокол № 8 від “31” серпня 2023 р.

Завідувач кафедри прикладної математики та інформатики

_____ (Наталія МАСЛОВА)

“31” серпня 2023 р.

Схвалено науково-методичною комісією галузі знань 12 Інформаційні технології

Протокол № 5 від “ 1” 09 2023р.

Голова _____
(підпис)

(Євген БАШКОВ)
(прізвище та ініціали)

1. Загальна інформація

Форма навчання	Денна
Статус	Базова
Обсяг в кредитах ЄКТС	6
Обсяг в годинах за навчальним планом, разом: в тому числі:	180
лекції:	48
лабораторні заняття:	32
самостійна робота:	100
Форма підсумкового контролю	Екзамен
Дисципліну викладають	Викладач проф. Дорогий Я.Ю., yaroslav.dorohyi@donntu.edu.ua

Передумови для вивчення дисципліни: успішному вивченню дисципліни «Безпека та захист операційних систем» сприяє попереднє опанування такими дисциплінами, як «Основи інформаційної безпеки», «Операційні системи».

2. Мета та предмет вивчення навчальної дисципліни «Безпека та захист операційних систем»

Навчальна дисципліна "Безпека та захист операційних систем" спрямована на забезпечення студентів необхідними знаннями та практичними навичками у галузі захисту інформації, що оброблюється операційними системами. Ця інформація включає в себе технічні та організаційні механізми захисту, що становлять невід'ємну частину операційних систем. Переважно, навчальна дисципліна відповідає нормативним вимогам освітньо-професійної програми.

Метою цієї навчальної дисципліни є формування у студентів навичок аналізування проблем і загроз безпеці програмного забезпечення, які виникають під час обробки інформації в інформаційно-комунікаційних системах. Також метою є надання студентам здатностей до обґрунтованого вибору засобів захисту для операційних систем відповідно до вимог національних та міжнародних стандартів. Ця дисципліна також спрямована на розвиток умінь налаштовувати засоби захисту в операційних системах та оцінювати рівень захищеності інформації відповідно до встановлених критеріїв.

Основні завдання лабораторних занять включають у себе ознайомлення студентів із сучасними засобами захисту інформації в операційних системах, а також надання їм навичок щодо їх застосування для вирішення практичних завдань з реалізації політик безпеки операційних систем. Також проводиться перевірка і моніторинг рівня захищеності інформації з використанням вітчизняних і міжнародних критеріїв оцінювання.

Компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання:

- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій;
- розробляти та аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;
- застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем;
- здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах;
- виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і/або кібербезпеки в інформаційно-телекомунікаційних системах.
- забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;
- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
- виконувати розробку експлуатаційної документації на комплексів засобів захисту;
- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої

політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

- вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації;

- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах

- проектувати та реалізовувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації;

- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

- визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах;

- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем;

- забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно-телекомунікаційних системах;

- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

- аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах;

- аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

3. Очікувані результати навчання

Основними результатами опанування дисципліни «Безпека та захист операційних систем» є вміння:

- забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань,

щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах

- вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки;

- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

- забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;

- здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;

- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

- забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

- забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах

Внаслідок вивчення курсу студенти повинні:

знати:

- основи розроблення захищених операційних систем;
- стандарти оцінювання захищеності операційних систем;
- законодавство України, яке регулює дану галузь;
- міжнародні стандарти, зокрема ISO/IEC 15408.

вміти:

- застосовувати отримані навички самостійного вивчення навчальної та наукової літератури, володіти понятійним апаратом;
- конфігурувати та використовувати для розв'язання задач засоби захисту ОС Windows;
- конфігурувати та використовувати для розв'язання задач засоби захисту ОС Linux;

- конфігурувати та використовувати для розв'язання задач засоби захисту ОС Android;
- конфігурувати та використовувати для розв'язання задач засоби захисту ОС IOS.

4. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання при опануванні дисципліною «Безпека та захист операційних систем» передбачено:

- екзамен;
- індивідуальні завдання з лабораторних робіт.

5. Критерії оцінювання результатів навчання

Максимальний бал, визначений схемою оцінювання, наведеною нижче, можливо отримати за умови своєчасного та правильного виконання завдань. За наявності помилок або при несвоєчасному виконанні оцінка знижується до 60% від максимальної.

Л1	Л2	Л3	Л4	Л5	Л6	Л7	Л8	Л9	Л10	Л11	Л12	Л13	Поточний контроль	Іспит	Max
4	4	4	5	4	5	4	5	5	5	5	5	5	60	40	100
3	3	2	3	2	3	2	3	3	3	3	3	3	36		

Примітки: 1) Л1, Л2 і т. д. лабораторні роботи;

2) У чисельнику максимальний бал – при своєчасному та правильному виконанні, у знаменнику – мінімальний (при правильному, але несвоєчасному виконанні)

Відповідність між шкалами встановлюється наступним чином:

Оцінка	
За 100-бальною шкалою	Для екзамену, курсового проекту (роботи), практики, диференційованого заліку, кваліфікаційного екзамену, випускної кваліфікаційної (дипломної) роботи (проекту)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

6. Програма навчальної дисципліни

6.1. Основні теми дисципліни

Змістовний модуль 1. Основи безпеки та захисту операційних систем.

Тема 1. Мета, задачі, зміст курсу. Основні визначення.

Тема 2. Модель загроз для операційної системи.

Змістовний модуль 2. Розроблення захищених операційних систем.

Тема 3. Розроблення захищених операційних систем.

Тема 4. Стандарти оцінювання захищеності операційних систем.

Змістовний модуль 3. Нормативно-правове регулювання галузі

Тема 5. Нормативно-правове регулювання в Україні.

Тема 6. Стандарт ISO/IEC 15408.

Змістовний модуль 4. Засоби захисту операційних систем.

Тема 7. Засоби захисту ОС Windows.

Тема 8. Засоби захисту ОС Linux.

Тема 9. Архітектура безпеки і механізми захисту Android.

Тема 10. Архітектура безпеки і механізми захисту IOS.

6.2. Теми лабораторних занять

№ п/п	Тема і зміст лабораторних занять	Обсяг лабораторних занять (ак. год.) для денної форми навчання
1	Лабораторна робота 1 (Теми 1-2, 8). Створення віртуальної машини в VirtualBox .	2
2	Лабораторна робота 2 (Теми 7). Механізми захисту в ОС Windows.	2
3	Лабораторна робота 3. (Теми 8). Управління файловою системою Linux .	2
4	Лабораторна робота 4. (Теми 8). Утиліти в Linux .	2
5	Лабораторна робота 5. (Теми 8). Архівне копіювання в Linux .	2
6	Лабораторна робота 6. (Теми 8). Secure Shell (SSH) та основні демони LINUX .	2
7	Лабораторна робота 7. (Теми 8). Firewall та управління його роботою (iptables та shorewall).	4
8	Лабораторна робота 8. (Теми 8). Автоматизація роботи та написання скриптів в BASH .	4
9	Лабораторна робота 9. (Теми 8). Розгортання та налаштування LDAP .	2
10	Лабораторна робота 10. (Теми 8). Розгортання та налаштування Kerberos .	2
11	Лабораторна робота 11. (Теми 7). Налаштування Active Directory .	2
12	Лабораторна робота 12. (Теми 9). Налаштування механізмів захисту Android (SELinux , App Sandbox та інш.).	2
13	Лабораторна робота 13. (Теми 10). Налаштування механізмів захисту iOS (Sandboxing , Secure Enclave та інш.).	4
	Всього лабораторних занять	32

6.3. Теми практичних занять

Не передбачено навчальним планом

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин для денної форми навчання
1	Тема 1. Мета, задачі, зміст курсу. Основні визначення.	2
2	Тема 2. Модель загроз для операційної системи.	4
3	Тема 3. Розроблення захищених операційних систем.	4

4	Тема 4. Стандарти оцінювання захищеності операційних систем.	4
5	Тема 5. Нормативно-правове регулювання в Україні.	4
6	Тема 6. Стандарт ISO/IEC 15408.	4
7	Тема 7. Засоби захисту ОС Windows.	16
8	Тема 8. Засоби захисту ОС Linux.	30
9	Тема 9. Архітектура безпеки і механізми захисту Android.	16
10	Тема 10. Архітектура безпеки і механізми захисту IOS.	16
	Разом	100

6.5. Індивідуальне завдання

Не передбачено навчальним планом

7. Література

7.1. Основна

1. М. В. Грайворонський, О. М. Новіков. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BVH, 2009. – 608 с.
2. Бондаренко М.Ф., Качко О.Г. Операційні системи. Навч. посібник. – Х.: Компанія СМІТ, 2018. – 432 с. ISBN 978-966-2028-02-7.
3. Яковина В.С. Операційні системи. Конспект лекцій. – Національний Університет "Львівська політехніка", Львів, 2016. 128 с.
4. Авраменко В. С., Авраменко А. С. Основи операційних систем. Навчальний посібник. – Черкаси: ЧНУ імені Богдана Хмельницького, 2018. – 524 с.: іл. ISBN 966-552-157-8.
5. Глоба Л.С. Розробка інформаційних ресурсів та систем. Том 1: Розподілені системи. – [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/uploads/l_1690_29298415.pdf
6. Глоба Л.С. Розробка інформаційних ресурсів та систем. Том 2: Розподілені системи. – [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/uploads/l_1690_27125554.pdf

7.2. Додаткова

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
2. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
4. Seth T. Ross. UNIX System Security Tools. – McGraw-Hill, 2000. – 444 p.

7.3. Методична

1. Безпека та захист операційних систем. Конспект лекцій. [Електронне видання] / Уклад.: Я.Ю. Дорогий. – Л.: ДВНЗ «ДонНТУ», 2023.
2. Безпека та захист операційних систем. Методичні вказівки до виконання лабораторних занять. Ч.І. [Електронне видання] / Уклад.: Я.Ю. Дорогий. – Л.: ДВНЗ «ДонНТУ», 2023.
3. Безпека та захист операційних систем. Методичні вказівки до виконання лабораторних занять. Ч.ІІ. [Електронне видання] / Уклад.: Я.Ю. Дорогий. – Л.: ДВНЗ «ДонНТУ», 2023.

4. Безпека та захист операційних систем. Методичні вказівки до виконання лабораторних занять. Ч.ІІ. [Електронне видання] / Уклад.: Я.Ю. Дорогий. – Л.: ДВНЗ «ДонНТУ», 2023.

5. Безпека та захист операційних систем. Методичні вказівки до організації самостійної роботи студентів. [Електронне видання] / Уклад.: Я.Ю. Дорогий. – Л.: ДВНЗ «ДонНТУ», 2023.

6. Безпека та захист операційних систем. Методичні вказівки до складання іспиту з дисципліни. [Електронне видання] / Уклад.: Я.Ю. Дорогий. – Л.: ДВНЗ «ДонНТУ», 2023.

8. Інформаційні ресурси

1. Operating System Fundamentals. – [Електронний ресурс] – Режим доступу: <https://www.coursera.org/programs/program-natsional-nii-tiekhnichnii-univiersitiet-ukrayini-kiyivs-kii/learn/akamai-operating-systems>.

2. Linux Server Management and Security. - [Електронний ресурс] – Режим доступу: <https://www.coursera.org/programs/program-natsional-nii-tiekhnichnii-univiersitiet-ukrayini-kiyivs-kii/learn/linux-server-management-security>.

3. Windows Server Management and Security. - [Електронний ресурс] – Режим доступу: <https://www.coursera.org/programs/program-natsional-nii-tiekhnichnii-univiersitiet-ukrayini-kiyivs-kii/learn/windows-server-management-security>